Summary on “Hold the Door!
Fingerprinting Your Car Key to Prevent Keyless Entry Car Theft”

Lohitanvita Rompicharla

RUID: 211009876

Department of Electrical and Computer Engineering

Objective

Unethical use of technology has become a crisis these days as the technology is becoming fully automatic. The conventional way of locking/unlocking car doors using physical keys is inconvenient and prone to theft through key duplication. The latest technology involves keyless entry systems based on RF signal transmission, i.e., when the car key fob is in the vicinity of the vehicle, door automatically unlocks on user command hence removing the inconvenience and making it more secure. But this automation is exposed to a wide range of attacks like signal-relaying, cryptographic, rolljam etc. Though there are many approaches like rolling codes, distance-bounding protocol, RF-PUF (RF finger printing) for preventing these attacks, they are all bound to functional limitations such as external communication system addition, easy decryption, working only for line of sight and indoor conditions. This research paper "Hold the Door!" (HODOR) uses RF fingerprinting technique without any modification to the current authentication system by successfully achieving false negative rate (FNR) as 0% and false positive rate (FPR) as 0.27% in all indoor/ outdoor conditions.

Introduction

There are two distinct keyless entry systems namely Remote Keyless Entry (RKE) system, and Passive Keyless Entry and Start (PKES) System. In RKE system, UHF-band (315MHz/433.92MHz/868MHz) signal is transmitted from key fob whose ID is then decrypted by vehicle's system to unlock the door. In PKES system a periodic LF band (125- 135kHz) signal is sent from the vehicle and if the corresponding key fob is in the vicinity of 1-2m, responds to the request through UHF signal and on user command the door unlocks. So, prediction and verification of UHF-band signals transmitted from key fob to the vehicle is the crucial part to avoid any attacks. The authors of the paper have clearly analyzed and mentioned the various types of attacks on keyless entry systems such as Single-band relay attack, Dual-band relay attack, Cryptographic attack, and attacks on RKE system. In Single-band relay attack, an attacker can relay the LF-band (RFID) signal sent by a vehicle to a range upto ~ 200m (nearly UHF-band range) and get the key fob to respond to the request by directly transmitting UHF-band signal to the vehicle. The Dual-band relay attack is attempted in two ways: Amplification attack, and Digital relay attack. In this case an external signal-extending module is used to relay both LF-band and UHF-band RF signals. For amplification attack, the adversaries amplify both LF band and UHF band signals using RF amplifier and inject the amplified signal from key fob directly into the vehicle. For Digital relay attack, the adversaries demodulate and decode the LF/UHF- band signals to deliver the created binary signal through Wi-Fi/ Bluetooth, then this received attack signal is encoded and modulated to inject into the vehicle. In the cryptographic attack, an adversary performs cryptanalysis with the obtained challenge-response pair signals to extract the long-term secret key. For Attacks on RKE systems, cryptographic attack where the encrypted secret-key between key fob and vehicle is compromised and Rolljam where signal from key fob is jammed and played back by the attacker to misuse it to unlock the doors are the two main categories. These attacks can be overcome by 'HODOR', which is a sub-authentication system that equips an RF receiver mounted on Body Control Module (BCM) of a car that controls CAN (unlocking), LIN (locking) functions. HODOR distinguishes the legitimate signal from malicious one and raises an attack detection alarm indicating BCM not to transmit CAN packet for unlocking a car door.

Working

The working of HODOR is dependent on a classifier created by authentic signals through a series of operations conducted in phases. HODOR contains two phases namely Training phase and Attack Detection phase. In Training phase, initially a set of legitimate UHF-band signals from the genuine key fob are collected and stored as a dataset, this dataset is then preprocessed by passing through band-pass filter to get meaningful information from baseband signal s(t) i.e., $r[t] \otimes c[t] = s[t] + n[t] \otimes c[t]$. This obtained baseband signal s(t) is demodulated into a pulse signal d(t) and encoded into a binary code by applying Frequency Shift Keying (FSK) and Amplitude Shift Keying (ASK) modulation techniques and normalized using RMS normalization $d_{RMS}[t] = d[t]/\sqrt{\sum_{i=1}^{N} d_i^2}$ for achieving noiseless received signal strength. The next step is feature extraction, a feature selection algorithm is

run to select the statistical features for both FSK and ASK modulation schemes. The salient features extracted by HODOR are (i) Peak Frequency (fpeak = arg max |DRMS[f]|), (ii) Carrier frequency offset ($f_c^{offset} = f_c' - f_c''$), (iii) signal-to-noise ratio ($SNR_{dB} = 10 \log_{10} P_{signal} / P_{noise}$) that lets us analyze the distance between key fob and vehicle, (iv) Kurtosis (= $E[(\mathrm{drms} - \mu/\sigma)^4]$), measure of peakedness of the sample signal in the time domain, (v) Spectral brightness, the amount of spectral energy corresponding to frequencies higher than a given cut-off threshold ($\sum_{f=fth}^{0.5*fs} |Drms[f]|^2$) where $f_{th} = 0.1*f_s$. These statistical features from the preamble of the obtained pulse signal are used to train a one-class classifier via semi-supervised learning for distinguishing legitimate signal from the attack signal. This trained signal then undergoes Normalization Parameter Calculation process that makes it ready for phase two of Attack Detection. For phase 2, a PKES system attack detection algorithm is followed that decides if the new signal from the classifier is from authorized key fob or not based on the normalized output and threshold value, if the normalized output is greater than the threshold, then it is considered a malicious attempt and door unlock request is not validated, alerting the BCM module.

Evaluation and Setup

HODOR is evaluated for the above-mentioned attacks and various environmental factors such as temperature variations, NLoS conditions, battery ranging. The hardware setup consists of two Software-Defined Radio (SDR) devices: 1) HackRF one, 2) Universal Software Radio Peripheral (USRP) for transmission and acquisition of UHF band RF signals, and GNU radio. This experimental setup was considered for two PKES system cars: 1) Kia Soul (with FSK modulation, center frequency 433.92MHz, frequency deviation 30KHz), 2) Volkswagen Tiguan (with ASK modulation, center frequency 433.92MHz), where the parameters for testing were: 1) Bandpass filter: high cut-off-15kHz, low cut-off- 45kHz, transition width- 10kHz, 2) ASK modulation for Tiguan car key fob: bit rate-3.5kbps, baseband signal- 7kHz, 3) cut-off frequency of LPF for Kia Soul-20kHz, 4) SMA cable, loop antenna for relay attack and three RF amplifiers for amplification attack simulations. Considering this experimental setup, the results were calculated using classification algorithm i.e., one-class Support Vector Machine (SVM) and k-nearest neighbors (k-NN) algorithms with threshold(γ) for testing 100 legitimate signals and 100 attack signals. The performance metrics are true positive rate (TPR), true negative rate (TNR), false positive rate (FPR), and false negative rate (FNR) with an aim of achieving FNR as 0%. The below stated are the results obtained: A) Single-Band Relay Attack Detection: SVM, k-NN ($\gamma = 4{,}5$) as a function of distance (5m, 10m, 15m) with FPR: 0%, FNR: 0%, B) Dual-Band Relay Attack Detection: i) Amplification attacks: SVM, k-NN as a function of amplifiers (20 – 25m) with FPR: 0%, FNR: 0%, ii) Digital relay attacks and Playback Attack Detection: SVM, k-NN ($\gamma = 70$) as a function of devices used in simulation, 1) Kia soul: SDR1: FPR 0.65%, FNR 0%, SDR2: FPR 0.27%, FNR 0%, 2) Volkswagen Tiguan: FPR 0%, FNR 0% , C) Non-Line-of-sight (NLoS) conditions: SVM, k-NN ($\gamma = 4{,}5$) as a function of key fob placement, i) Key fob in backpack: FPR 1.32% and 1.35%, FNR 0%, ii) Key fob in pocket: FPR 1.71% and 1.67%, FNR 0%, D) Attack Detection in RKE systems: experiment conducted with 3 Key fobs and there features were extracted for both cryptographic and playback attacks, and did not yield FPR, FNR as 0%. E) Effects of Temperature Variations: tested in an ice box with dry ice, SVM, k-NN as a function of temperature (20°C to -20°C) with FPR: 6.36%, FNR: 0.65%, F) Battery aging: Panasonic CR2032 lithium battery was used till its voltage decreased from 3V to 2.5V, SVM, k-NN as a function of voltage level gives FPR 0% but does not operate properly due to insufficient voltage supply, G) Execution Time: Considering Raspberrypi 3B single-board computer as a reference hardware platform, the total operation time for i) PKES system with FSK modulation is 163.8ms (k-NN) and 159.038ms (SVM), ii) RKE system with FSK modulation is 12.8ms (k-NN) and 9.04ms (SVM), iii) PKES system with ASK modulation is 126.27ms (k-NN) and 121.37ms (SVM), and iv) RKE system with ASK modulation is 15.13ms (k-NN) and 11.2ms (SVM). H) Feature Importance for attack scenario is obtained using Relief algorithm and tabulated, I) Advanced Dual-Band Relay Attacks: Equipping with analog filters or SDR devices with a high sample rate, obtained FNR and FPR as 0% for Amplification attack but could not impersonate a legitimate signal

for Playback attack. J) Dynamic channel Conditions: Obtained a decent FPR and FNR in dynamic conditions like underground parking lot and roadside parking during most crowded hours.

Results

From the results of evaluation of HODOR, we can agree that HODOR is effective in detecting above defined simulated attacks by reducing false negative rate occurrence. The experiment setup and outcome are also found suitable for a number of salient features under channel conditions, path loss, noise signals, multipath signals, temperature variation, battery aging and NLoS conditions indicating its efficiency in real time environmental conditions.

Conclusion

Examining all the above-mentioned consequences and effects, we can conclude that HODOR is a highly efficient, cumbersome free system for preventing keyless entry car theft that supports manufacture-installed support systems without extra hardware addition. Though it has depicting amazing outputs for single-band, dual-band, playback attack detection with least erroneous detection occurrences, it still has scope for improvement in execution time, battery aging, dynamic channel conditions and advanced dual-band relay attack detection since it is getting affected by external factors producing weaker performance results.

Future Scope

Given all the advantages and disadvantages of ‘HODOR’ system, we can acknowledge that it is safe and secure to utilize the HODOR system currently. Also, the discussion section of this paper indicates that HODOR cannot perfectly impersonate the legitimate signal in case of ADC and DAC processes, and yet to study further for practical issues and scalability.